UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* SUBJECT PREMISES/PERSONS/VEHICLES	)	Case No. MJ23-572

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SUBJECT PREMISES/PERSONS/VEHICLES, more fully described in Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252(a)(2), 2252 (a)(4)(B)	Receipt/Distribution of Child Pornography, Possession of Child Pornography

The application is based on these facts:

✓ See Affidavit, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

JESSE D MILLER Digitally signed by JESSE D MILLER Date: 2023.11.28 14:12:35 -08'00'

Applicant's signature

Jesse Miller, Special Agent

Printed name and title

◯ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 11/30/2023

Paula L McCandlis

Judge's signature

City and state: Seattle, Washington

Paula L. McCandlis, United States Magistrate Judge

Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
WHATCOM COUNTY)

I, Jesse Miller, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), assigned to the Assistant Special Agent in Charge (ASAC) Blaine, Washington, field office. I have been employed as an HSI Special Agent since 2001. In my capacity as a Special Agent, I am responsible for conducting investigations into the numerous federal laws enforced by HSI. Since 2018, I have investigated criminal violations relating to child exploitation and child pornography, including violations pertaining to the unlawful production, importation, distribution, receipt, attempted receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC), Special Agent Training Program and have received further specialized training in investigating child pornography and child exploitation crimes. My training included courses in law enforcement techniques, federal criminal statutes, conducting criminal investigations, and the execution of search warrants. I have participated in the execution of many search warrants which involved child exploitation and/or child pornography offenses and the search and seizure of computers and other digital devices. I am a member of the Internet Crimes Against Children (ICAC) Task Force in the Western District of Washington, and work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

of children. In April of 2018, I completed a ICAC sponsored training for the BitTorrent (P2P) file sharing program.

PURPOSE OF THE AFFIDAVIT

2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the following:

a. 4808 Grove St, Apt 8, Marysville, WA, 98270 (the SUBJECT PREMISES)

b. The person of Mark Garcia (SUBJECT PERSON 1),

c. The person of Eric Garcia (SUBJECT PERSON 2)

d. 2016 Toyota Corolla, with Washington License Plate # CCT0084, (SUBJECT VEHICLE 1)

e. 2015 Ford Explorer, with Washington License Plate #CAZ6550 (SUBJECT VEHICLE 2)

3. As set forth below, there is probable cause to believe that the SUBJECT PREMISES, SUBJECT PERSONS, and/or SUBJECT VEHICLES will contain evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. § 2252(a)(2), (b)(1) (Receipt/Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B), (b)(2) (Possession of Child Pornography), as well as attempt/conspiracy to commit such offenses, the TARGET OFFENSES. I seek authorization to search and seize the items specified in Attachment B, which is incorporated herein by reference.

4. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

5. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are relevant to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), will be found at the SUBJECT PREMISES.

PEER-TO-PEER (P2P) FILE SHARING

6. Peer to peer (P2P) file sharing is a method of communication available to internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to transfer digital files from one computer system to another while connected to a network, usually on the internet. There are multiple types of P2P file sharing networks on the internet. To connect to a particular P2P file sharing network, a user first obtains a P2P client software program for a particular P2P file sharing network, which can be downloaded from the internet. A particular P2P file sharing network may have many different P2P client software programs that allow access to that particular P2P file sharing network. Additionally, a particular P2P client software program may be able to access multiple P2P file sharing networks. These P2P client software share common protocols for network access and file sharing. The user interface, features, and configurations may vary between clients and versions of the same client.

7. In general, P2P client software allows the user to set up file(s) on a computer to be shared on a P2P file sharing network with other users running compatible P2P client software. A user can also obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

8. Some P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.

9. Typically, during a default installation of a P2P client software program, settings are established which configure the host computer to share files. Depending upon the P2P client software used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed.

10. Typically, a setting establishes the location of one or more directories or folders whose contents (digital files) are made available for distribution to other P2P clients. In some clients, individual files can also be shared.

11. Typically, a setting controls whether or not files are made available for distribution to other P2P clients.

12. Typically, a setting controls whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of the file segments on the network for distribution.

13. Typically, files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value is computed for each file and/or piece of a file being shared (dependent on the P2P file sharing network), which uniquely identifies it on the network. A file (or piece of a file) processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their file names. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, typically, users may receive a selected file from numerous sources by accepting segments of the same file

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. This client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same files are used during this process.

14. P2P file sharing networks, including the BitTorrent network, are frequently used to trade digital files of child pornography. These files include both images and movie files.

15. The BitTorrent network is a very popular and publicly available P2P sharing network. Most computers that are part of this network are referred to as "peers." The terms "peers" and "clients" can be used interchangeably when referring to the BitTorrent network. A peer can simultaneously provide files to some peers while downloading files from other peers.

16. The BitTorrent network can be accessed by computers running many different client programs, some of which include the BitTorrent client program, uTorrent client program, and Vuze client program. These client programs are publicly available and free P2P client software programs that can be downloaded from the internet. There are also BitTorrent client programs that are not free. These BitTorrent client programs share common protocols for network access and file sharing. The user interfaces, features, and configuration may vary between clients and versions of the same client.

17. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files. Depending upon the BitTorrent client used, a user may have the ability to reconfigure some of those settings during installation or after installation has been completed. Typically, a setting establishes the location of one or more directories of folders whose contents (files) are made available to other BitTorrent network users to download.

18. In order to share a file or set of files on a BitTorrent network, a "Torrent" file needs to be created by the user that initially wants to share the file or set of files. A

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

"Torrent" is typically a small file that describes the file(s) that are being shared, which may include information on how to locate the file(s) on the BitTorrent network. A typical BitTorrent client will have the ability to create a "Torrent" file. It is important to note that the "Torrent" file does not contain the actual file(s) being shared, but information about the file(s) described in the "Torrent," such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent." The "info hash" is a SHA-1 hash value of the set of data describing the file(s) referenced in the "Torrent," which include the SHA-1 hash value of each piece, the file size, and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers." "Trackers" are computers on the BitTorrent network that collate information about peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the "Torrent." It is important to note that the "Trackers" do not actually have the file(s) and are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

19. Once a "Torrent" is created, in order to share the file(s) referenced in the "Torrent" file, a user typically makes the "Torrent" available for other users, such as via websites on the Internet.

20. In order to locate "Torrent" files of interest, a typical user will use keyword searches within the BitTorrent network client itself or on websites hosting "Torrents." Once a "Torrent" file is located that meets the keyword search criteria, the user will download the "Torrent" file to their computer. Alternatively, a user can also search for

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

and locate "magnet links," which is a link that enables the BitTorrent network client program itself to download the "Torrent" to the computer. In either case, a "Torrent" file is downloaded to the user's computer. The BitTorrent network client will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent," to include the remote peers/clients Internet Protocol (IP) addresses.

21. For example, a person interested in obtaining child pornographic images on the BitTorrent network would open the BitTorrent client application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." (It should be noted that this search term may not have been used in this investigation.) The results of the torrent search are typically returned to the user's computer by displaying them on the torrent hosting website. The hosting website will typically display information about the torrent, which can include the name of the torrent file, the name of the file(s) referenced in the torrent file, the file(s) size, and the "info hash" SHA-1 value of the torrent file. The user then selects a torrent of interest to download to their computer. Typically, the BitTorrent client program will then process the torrent file. The user selects from the results displayed the file(s) they want to download that were referenced in the torrent file. Utilizing trackers and other BitTorrent network protocols (such as Distributed Hash Tables, Peer Exchange, and Local Peer Discovery), peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the torrent file available for sharing. The file(s) is then downloaded directly from the computer(s) sharing the file. Typically, once the BitTorrent network client has downloaded part of the

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

file(s), it may immediately begin sharing the file with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 piece hash described in the torrent file. During the download process, a typical BitTorrent client program displays the Internet Protocol address of the peers/clients that appear to be sharing part or all of the file(s) referenced in the torrent file or other methods utilized by the BitTorrent network protocols. The downloaded file is then stored in the area previously designated by the user and/or the client program. The downloaded file(s), including the torrent file, will remain until moved or deleted.

22. Law Enforcement has created BitTorrent network client programs that obtain information from trackers about peers/clients recently reporting that they are involved in sharing digital files of known actual child pornography (based on the "info hash" SHA-1 hash value), which then allows the downloading of a file from a single IP address (as opposed to obtaining the file from multiple peers/clients on the network.) This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography on the BitTorrent network.

23. During the query and/or downloading process from a remote BitTorrent network client, certain information may be exchanged between the investigator's client and the remote client they are querying and/or downloading a file from. Such as 1) the remote client's IP address; 2) a confirmation from the remote client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the remote client program; and 3) the remote client program and version. This information may remain on the remote client's computer system for long periods of time. The investigator has the ability to log this information. A search can later be conducted on a seized computer system(s) for this information, which may provide further evidence that the investigator's client communicated with the remote client.

24.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

SUMMARY OF PROBABLE CAUSE

25. Between August 5, 2023, and October 6, 2023, I used a law enforcement version of BitTorrent to identify P2P users possessing and distributing image and video files depicting child pornography. I used the law enforcement version of BitTorrent to download files depicting child pornography from a P2P user at IP address 73.181.150.252 (the SUBJECT IP ADDRESS). The undercover downloads are detailed below.

26. August 5, 2023, at approximately 2:20 a.m. PST, I used the law enforcement version of BitTorrent to establish a single source connection with a P2P user at the SUBJECT IP ADDRESS, who was determined to be in possession of suspected child pornography. Among the files downloaded from the SUBJECT IP ADDRESS was the following file that I reviewed and describe below:

> **File:** This photo depicts a naked prepubescent female and an adult male. An adult male penis is in the child's mouth. Given her small stature, lack of pubic hair/muscular development, and youthful appearance, I estimate this young girl is between six and eight years old.

27. On October 6, 2023, at approximately 4:08 a.m. PST, I used the law enforcement version of BitTorrent to establish a single source connection with a P2P user at the SUBJECT IP ADDRESS, who was determined to be in possession of suspected child pornography. Among the files downloaded from the SUBJECT IP ADDRESS were the following video, which I reviewed and describe below:

> **File:** This video is approximately 2 minutes and 17 seconds long and depicts a naked prepubescent female and an adult male. The adult male has vaginal sex with the child. The child has the words "Fuck Me" written on the child's chest, along with an arrow pointing towards the child's vagina. The video ends with an adult male ejaculating on the female's face. Given her small stature, lack of pubic

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

development and body hair, and youthful appearance, I estimate the young girl is between seven and nine years old.

28. A query of a publicly available database revealed the SUBJECT IP ADDRESS belonged to Comcast. In response to a summons seeking subscriber information for the SUBJECT IP ADDRESS, Comcast reported that the SUBJECT IP ADDRESS was assigned to Mark Garcia with a service address at the SUBJECT PREMISES during the times when I used the law enforcement version of BitTorrent to download the files described above.

29. Law enforcement conducted surveillance at the SUBJECT PREMISES, which is an apartment building, and observed two vehicles parked on the property parking lot. The vehicles were a Toyota Corolla (SUBJECT VEHICLE 1) which is registered to Mark Garcia, and a black Ford Explorer (SUBJECT VEHICLE 2) which is registered to Eric Garcia.

30. Washington State Department of License records show that Mark Garcia and Eric Garcia both have valid driver licenses that list the SUBJECT PREMISES as their current residential address.

31. Washington State Department of License records show that SUBJECT VEHICLES 1 and 2 are currently registered to, Mark Garcia and Eric Garcia, respectively. Both are registered at the SUBJECT PREMISES. No other subjects have been seen at the SUBJECT PREMISES.

32. Based on my investigation to date, Mark Garcia and Eric Garcia appear to be the only residents at the SUBJECT PREMISES. They are both adults, and I believe they are brothers.

33. Based on my knowledge, training, and experience, and the experience of other law enforcement officers, I know that it is common for multiple individuals and computers within a residence to share Internet access. I believe that someone used at least one computer from the SUBJECT PREMISES to distribute child pornography via

an Internet based P2P file sharing program, and that evidence of that crime will be found in the SUBJECT PREMISES, SUBJECT PERSONS, and/or SUBJECT VEHICLES.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

34. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of

various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

35. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Importantly, e-mail and cloud storage can be a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers, which allow users to store a large amount of material at no cost, and possibly reducing the amount of any evidence of any of that material on the users' computer(s).

36. Even if such individuals use a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as set forth in Attachment

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

A, including on digital devices other than the portable device (for reasons including the frequency of "backing up" or "synching" mobile phones to computers or other digital devices).

37. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents, and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

38. Given the above-stated facts and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that the person who used computer at the SUBJECT PREMISES shared visual depictions of minors engaged in sexually explicit conduct likely has a sexualized interest in children and depictions of children and that the SUBJECT PREMISES, SUBJECT PERSONS, and/or SUBJECT VEHICLES is likely to contain evidence, fruits, and instrumentalities of the TARGET OFFENSES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

39. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found, in whatever form they are found. One form in which the **[evidence, fruits, and/or instrumentalities]** might be found is data stored on digital devices[1] such as computer hard drives or other electronic storage media.[2] Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B).

40. *Probable cause.* Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a digital device or other electronic storage media is found during the search of the SUBJECT PREMISES, SUBJECT PERSONS, and/or SUBJECT VEHICLES, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the TARGET OFFENSES will be stored on those digital devices or other electronic storage media. As noted above, I believe someone at the SUBJECT PREMISES used a computer to share child sexual abuse imagery online. There is, therefore, probable cause to believe that evidence, fruits and/or instrumentalities of the TARGET OFFENSES exists and will be

---

[1] [“Digital device” includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants (“PDAs”), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

found on digital devices or other electronic storage media found in a search of the SUBJECT PREMISES, SUBJECT PERSONS, and/or SUBJECT VEHICLES, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be preserved (and consequently also then recovered) for months or even years after they have been downloaded onto a storage medium, deleted, or accessed or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device or other electronic storage media, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

41. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how digital devices or other electronic storage media were used, the purpose

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital devices or other electronic storage media located at the search of the SUBJECT PREMISES, SUBJECT PERSONS, and/or SUBJECT VEHICLES because:

a. Stored data can provide evidence of a file that was once on the digital device or other electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the history of connections to other computers, the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device or other electronic storage media was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.[3] Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a digital device or other electronic storage media works can, after examining this forensic evidence in its proper context, draw conclusions about how the digital device or other electronic storage media were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device or other electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information

[3] For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device or other electronic storage media was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS

42. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of premises for information that might be stored on digital devices or other electronic storage media often requires the seizure of the physical items and later off-site review consistent with the warrant. In lieu of removing all of these items from the premises, it is sometimes possible to make an image copy of the data on the digital devices or other electronic storage media, onsite. Generally speaking, imaging is the taking of a complete electronic picture of the device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the item, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine the respective digital device and/or electronic storage media to obtain evidence. Computer hard drives, digital devices and electronic storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months,

depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Digital devices or other electronic storage media can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the items off-site and reviewing them in a controlled environment will allow examination with the proper tools and knowledge.

c. *Variety of forms of electronic media*. Records sought under this warrant could be stored in a variety of electronic storage media formats and on a variety of digital devices that may require off-site reviewing with specialized forensic tools.

SEARCH TECHNIQUES

43. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to this Affidavit, and will specifically authorize a later review of the media or information consistent with the warrant.

44. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain digital devices or other electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

45. Consistent with the above, I hereby request the Court's permission to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of Attachment B to this Affidavit, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

A. Processing the Search Sites and Securing the Data.

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at the subject premises described in Attachment A that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B to this Affidavit.[4]

c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the

[4] The purpose of using specially trained computer forensic examiners to conduct the imaging of digital devices or other electronic storage media is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, often lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is often important that computer forensic examiners and investigative personnel work closely together.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search locations described in Attachment A will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search locations described in Attachment A that have previously connected to devices at other locations may contain data from those other locations.

d. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

B. Searching the Forensic Images.

a. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

b. These methodologies, techniques and protocols may include the use of a "hash value" library to exclude normal operating system files that do not need to be further searched. OR - Agents may utilize hash values to exclude certain known files, such as the operating system and other routine software, from the search results.

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

CONCLUSION

46. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of the TARGET OFFENSES will be found during a search of the SUBJECT PREMISES, SUBJECT PERSONS, and/or SUBJECT VEHICLES as more fully described in Attachment A to this Affidavit, as well as on and in any digital devices or other electronic storage media found. I therefore request that the court issue a warrant authorizing a search of the SUBJECT PREMISES, SUBJECT PERSONS, and/or SUBJECT VEHICLES, as well as any digital devices and electronic storage media located therein, for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

47. The affidavit and application are being presented by reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41(d)(3).

JESSE D MILLER Digitally signed by JESSE D MILLER Date: 2023.11.28 14:15:24 -08'00'

Jesse Miller
Special Agent, HSI

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit this 30th day of November 2023.

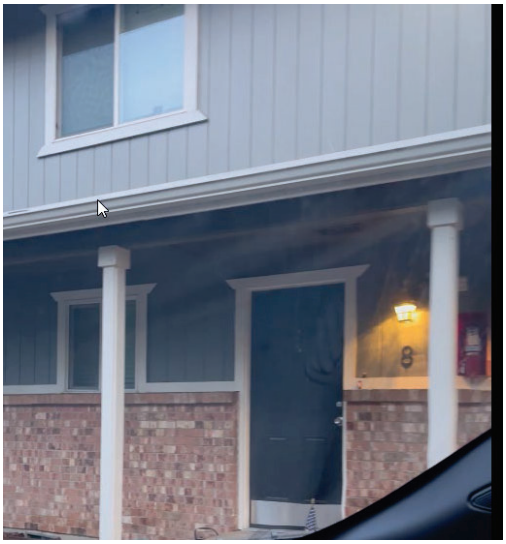
PAULA L. MCCANDLIS
United States Magistrate Judge

UNITED STATES ATTORNEY
700 Steward Street, Suite 5220
Seattle, WA 98101
206-553-7790

ATTACHMENT A

Description of Property to be Searched

The SUBJECT PREMISES is Apartment 8 within the multi-unit apartment building located at 4808 Grove St, Marysville, WA, 98270. The property consists of two separate buildings. Apartment 8 is located on the south side of the complex with the front door facing south. Half of the first-floor exterior wall is brick, and the other half appears gray. The first floor has a short-extended roof that extends to the sidewalk, approximately 2-3 foot, covering the front door.



The search is to include the entirety of Apartment 8 and any parking/garage/storage space(s) exclusively assigned to that unit, and any digital device(s) or other electronic storage media found.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUBJECT PERSONS

Mark Anthony Garcia Jr., DOB: XX/XX/1985, Height 5'6", Weight 250 (SUBJECT PERSON 1)

Eric James Garcia, DOB: XX/XX/91, Height 5'9", Weight 260 (SUBJECT PERSON 2)

The search is to include the SUBJECT PERSONS and any backpacks, bags, or other containers that the SUBJECT PERSONS may be capable of carrying, as well as any digital devices or electronic storage media found.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Description of the SUBJECT VEHICLES

2016 Toyota Corolla, with Washington License Plate # CCT0084, (SUBJECT VEHICLE 1)


2015 Ford Explorer, with Washington License Plate #CAZ6550, (SUBJECT VEHICLE 2)


The search is to include the entirety of the SUBJECT VEHICLES and any closed containers found therein, as well as any digital devices or electronic storage media found.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, and magnetic form (such as tapes, cassettes, hard disks, floppy disks, diskettes, compact discs, CD-ROMs, DVDs, optical discs, Zip cartridges, printer buffers, smart cards, or electronic notebooks, or any other electronic storage medium) that constitute evidence, instrumentalities, or fruits of violations of violations of 18 U.S.C. § 2252(a)(2), (b)(1) (Receipt/Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B), (b)(2) (Possession of Child Pornography), as well as attempt/conspiracy to commit those offenses (the TARGET OFFENSES):

1. Documents, records, and things that constitute evidence of who exercises dominion and control over the SUBJECT PREMISES.

2. All records relating to violations of the TARGET OFFENSES, including:

3.

a. visual depictions of minors engaged in sexually explicit conduct

b. identifying information for any individuals shown in such depictions or evidence that would otherwise assist in the identification of those depicted or those responsible for creating such visual depictions

c. information concerning the possession, receipt, distribution, or production of visual depictions of minors engaged in sexually explicit conduct

d. information identifying the source of any visual depictions of minors engaged in sexually explicit conduct

e. evidence of communications related to the possession, receipt, distribution, or production of visual depictions of minors engaged in sexually explicit conduct

f. evidence of contact with or communications about minors

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

g. evidence indicative of a sexualized interest in minors or depictions of minors

h. evidence of the use of P2P filesharing programs.

4. Digital devices[5] or other electronic storage media[6] and/or their components, which include:

a. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

b. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

---

[5] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[6] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

5. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

f. evidence of the times the digital device or other electronic storage media was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

h. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

i. contextual information necessary to understand the evidence described in this attachment.

6. Records and things evidencing the use of the internet, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970